I claim

1. A cryptographic method, where a non-empty set **F** of encryption keys $\mathbf{F}_1, \mathbf{F}_2, \mathbf{F}_3, \ldots$ are associated with one single decryption key **B** satisfying $\boldsymbol{b}(\boldsymbol{f}(\mathbf{m}))=\mathbf{m}$ for any input **m** and for ***b*** being a decryption function employing **B** and for ***f*** being an encryption function employing any $\mathbf{F}_i \in \mathbf{F}$, comprising:

obtaining arbitrary and/or random input from which cryptographic keys are generated;

generating a decryption key;

generating one of a plurality of corresponding encryption keys;

supplying an encryptor with said encryption key;

accepting a message **m**;

encrypting **m** by said encryptor to ciphertext **c** using said encryption key;

supplying a decryptor with said decryption key; and

decrypting **c** by said decryptor to recover **m** using said decryption key.

2. A cryptographic method for establishing a secret between two parties comprising:

generating a secrecy primitive; and

establishing said secret between said two parties using said secrecy primitive.

3. A cryptographic method as in claim 1 comprising:

obtaining arbitrary and/or random input from which cryptographic keys are generated;

generating a decryption key;

generating a corresponding encryption key through a series of transforms where at least one of said transforms facilitates the introduction of arbitrary or random noise of any desired sufficient amount;

supplying an encryptor with said encryption key;

accepting a message **m**;

encrypting **m** by said encryptor to ciphertext **c** using said encryption key;

supplying a decryptor with said decryption key; and decrypting **c** by said decryptor to recover **m** using said decryption key.

4. A cryptographic method as in claim 1 comprising:

obtaining arbitrary and/or random input from which cryptographic keys are generated;

generating a decryption key including a set of parameters **p** in normal positional number representation;

generating a corresponding encryption key comprising:

converting **p** to self-contained components;

constructing encryption key parameters from said self-contained components by inserting zero or more arbitrary/random components in arbitrarily or randomly chosen component positions; and

generating all other encryption key parameters;

supplying an encryptor with said encryption key;

accepting a message **m**;

encrypting **m** by said encryptor to ciphertext **c** using said encryption key;

supplying a decryptor with said decryption key; and

decrypting **c** by said decryptor to recover **m** using said decryption key.

5. A cryptographic method, as in claim 1, adopting **n** integer functions $f_1, f_2, \ldots, f_n$ mapping from $[0, 2^h)$ to $[0, 2^h+\delta)$, where $h > 1$ and $2^h+\delta > 1$, comprising:

obtaining arbitrary and/or random input from which cryptographic keys are generated;

generating a decryption key, including the generation of a first set of positive integers $\mathbf{X} = \{\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n}\}$ and a second set of positive integers $\mathbf{W} = \{\mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_n}\}$ satisfying $\mathbf{x_i} > \beta_1\mathbf{x_1} + \beta_2\mathbf{x_2} + \ldots + \beta_{i-1}\mathbf{x_{i-1}} + \gamma_1\mathbf{w_1} + \gamma_2\mathbf{w_2} + \ldots + \gamma_i\mathbf{w_i}$ where, for $1 \leq \mathbf{i} \leq \mathbf{n}$, $\gamma_i = f_i(\beta_i)$ and $\beta_i \in [0, 2^h)$;

transforming **X** to $\mathbf{Y} = \{\mathbf{y_1}, \mathbf{y_2}, \ldots, \mathbf{y_n}\}$ and **W** to $\mathbf{U} = \{\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_n}\}$, including an optional permutation and one or more rounds of invertible strong modular multiplication; and further transforming $\mathbf{Y}$ to $\mathbf{Z} = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_n\}$ and $\mathbf{U}$ to $\mathbf{V} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ satisfying the following:

a. $\mathbf{p}_0, \mathbf{p}_1, \ldots, \mathbf{p}_{t-1}$ are pairwise co-prime

b. $\mathbf{z}_i = (\mathbf{z}_{i,0}, \mathbf{z}_{i,1}, \ldots, \mathbf{z}_{i,qt-1})$ for $1 \leq \mathbf{i} \leq \mathbf{n}$ and $\mathbf{q} \geq 1$

c. $\mathbf{J} = \{\mathbf{j}_0, \mathbf{j}_1, \ldots, \mathbf{j}_{k-1}\}$ is a set of arbitrary or random indices where $0 \leq \mathbf{j}_0, \mathbf{j}_2, \ldots, \mathbf{j}_{k-1} < \mathbf{t}$

d. $\mathbf{S} = \{\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}\}$ is an arbitrary or random set satisfying:

$0 \leq \mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1} < \mathbf{qt}$, and $\mathbf{S} \,\%\, \mathbf{t} = \{\mathbf{s}_0\%\mathbf{t}, \mathbf{s}_1\%\mathbf{t}, \ldots, \mathbf{s}_{k-1}\%\mathbf{t}\} = \mathbf{J}$

e. $\prod \mathbf{p}_{j \in J} > \beta_1 \mathbf{y}_1 + \beta_2 \mathbf{y}_2 + \ldots + \beta_n \mathbf{y}_n + \gamma_1 \mathbf{u}_1 + \gamma_2 \mathbf{u}_2 + \ldots + \gamma_n \mathbf{u}_n$

f. $\mathbf{z}_{i,s \in S} = \mathbf{y}_i \,\%\, \mathbf{p}_{s\%t}$

g. $\mathbf{z}_{i,s \notin S}$ are arbitrary or random numbers modulo $\mathbf{p}_{s\%t}$ for $0 \leq \mathbf{s} < \mathbf{qt}$

h. $\mathbf{v}_i = (\mathbf{v}_{i,0}, \mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,qt-1})$ for $1 \leq \mathbf{i} \leq \mathbf{n}$

i. $\mathbf{v}_{i,s \in S} = \mathbf{w}_i \,\%\, \mathbf{p}_{s\%t}$

j. $\mathbf{v}_{i,s \notin S}$ are arbitrary or random numbers modulo $\mathbf{p}_{s\%t}$ for $0 \leq \mathbf{s} < \mathbf{qt}$.

6. A cryptographic method as in claim 5 further comprising:

supplying an encryptor with said encryption key;

encrypting by said encryptor one or more **nh**-bit data blocks which are divided into **h**-bit sub-blocks $\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n$, where each block is encrypted to $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{qt-1})$ with $\mathbf{c}_s = (\mathbf{d}_1\mathbf{z}_{1,s} + \mathbf{d}_2\mathbf{z}_{2,s} + \ldots + \mathbf{d}_n\mathbf{z}_{n,s} + f_1(\mathbf{d}_1)\mathbf{v}_{1,s} + f_2(\mathbf{d}_2)\mathbf{v}_{2,s} + \ldots + f_n(\mathbf{d}_n)\mathbf{v}_{n,s}) \,\%\, \mathbf{p}_{s\%t}$ for $0 \leq \mathbf{s} < \mathbf{qt}$;

supplying a decryptor with said decryption key; and

decrypting by said decryptor each of said encrypted blocks **c** to recover said data blocks, by extracting $\mathbf{C} = \{\mathbf{c}_s \mid \mathbf{s} \in \mathbf{S}\}$ from **c** and by repeating, for each $\mathbf{d}_i$ for $1 \leq \mathbf{i} \leq \mathbf{n}$, the following:

a. converting **C** to a form where $\mathbf{d}_i$ can be determined

b. obtaining $\mathbf{d}_i$ from said converted **C**

c. removing from said converted **C** the quantity that $\mathbf{d}_i$ introduced.

7. A cryptographic method as in claim 6, where said encryption is carried out, in lieu, independently on self-contained components, comprising:

calculating **c** by carrying out two or more of said additions (+) and/or by computing two or more of said terms $\mathbf{d}_i\mathbf{z}_{i,j}$ and $f_i(\mathbf{d}_i)\mathbf{v}_{i,j}$ in parallel.

8. A cryptographic method, as in claim 1, for communicating a message securely from a first party **E** to a second party **D** comprising:

obtaining at party **D** arbitrary and/or random input from which cryptographic keys are generated;

generating at party **D** a decryption key to be kept secret;

generating at party **D** one of a plurality of corresponding encryption keys;

distributing said encryption key from party **D** to party **E**;

accepting a message **m** at party **E**;

encrypting **m** to ciphertext at party **E**, employing said encryption key;

transmitting said ciphertext from party **E** to party **D**;

receiving said ciphertext at party **D**; and

decrypting said ciphertext at party **D** to recover **m**, employing said decryption key.

9. A cryptographic method as in claim 8 further comprising:

applying chaining in the encryption of **m** to **c** with zero or more blocks of arbitrary or random bits pre-pended to **m**.

10. A cryptographic method, as in claim 5, using dynamic mapping for communicating a message securely from a first party **E** to a second party **D** which generates said encryption key to be kept secret and said decryption key to be sent to party **E**, further comprising:

agreeing upon a set of mapping functions $f_1, f_2, \ldots, f_n$ for said current communication by said two parties, where said set of mapping functions only observe their domain and range restrictions and are independent of and unrelated to any other encryption or decryption parameters;

distributing said encryption key from party **D** to party **E**;

accepting a message **m** at party **E**;

encrypting **m** to ciphertext at party **E**, employing said encryption key and $f_1, f_2, \ldots, f_n$;

transmitting said ciphertext from party **E** to party **D** over a communication channel;

receiving said ciphertext at party **D**; and

decrypting said ciphertext at party **D** to recover **m**, employing said decryption key and $f_1, f_2, \ldots, f_n$.

11. A cryptographic method, as in claim 2, where one encryption key $\mathbf{F}_x$ is associated with a non-empty set $\mathbf{B}_x$ of decryption keys $\mathbf{B}_{x,1}, \mathbf{B}_{x,2}, \ldots, \mathbf{B}_{x,n}$ satisfying $b_i(f(\mathbf{m})) \neq b_j(f(\mathbf{m}))$ for one or more input **m** if $i \neq j$, with b_i and b_j being decryption functions employing $\mathbf{B}_{x,i}$ and $\mathbf{B}_{x,j}$ respectively and f being an encryption function employing $\mathbf{F}_x$, comprising:

obtaining at a first party **D** arbitrary and/or random input from which cryptographic keys are generated;

generating at party **D** secret decryption keys $\mathbf{B}^1, \mathbf{B}^2, \ldots, \mathbf{B}^k$ where $\mathbf{B}^x \in \mathbf{B}_x$ for $1 \leq \mathbf{x} \leq \mathbf{k}$;

generating at party **D** encryption keys $\mathbf{F}_1, \mathbf{F}_2, \ldots, \mathbf{F}_k$ as said secrecy primitive, where $\mathbf{F}_x$ corresponds to $\mathbf{B}_x$ for $1 \leq \mathbf{x} \leq \mathbf{k}$;

distributing said encryption keys from party **D** to a second party **E**; and

establishing said secret between said two parties by making use of said encryption keys and decryption keys.

12. A cryptographic method, as in claim 11, for establishing said secret comprising:

generating at party **D** said encryption keys and decryption keys;

distributing said encryption keys from party **D** to party **E**;

receiving said encryption keys at party **E**;

encrypting arbitrary or random data blocks at party **E** employing said encryption keys;

transmitting said encrypted data blocks from party **E** to party **D** over a communication channel;

receiving at party **D** said encrypted data blocks from party **E**;

decrypting said encrypted data blocks employing said decryption keys at party **D** to obtain information/characteristics about said data blocks; and

communicating to party **E** by party **D**, based on said information/characteristics gained about said data blocks, instructions to transform a special entity to a form from which party **E** learns said secret party **D** intends to convey and establish.

13. A cryptographic method as in claim 12 further comprising:

using said established secret for further secure communications and cryptographic applications between said two parties.

14. A cryptographic method as in claim 1 for the zero-knowledge authentication/identification of a party possessing said secret decryption key comprising:

proving said authenticity/identity by said party through the exhibition of the ability to decrypt any valid encrypted messages using said decryption key.

15. A cryptographic system, where a non-empty set **F** of complete encryption keys $\mathbf{F_1}$, $\mathbf{F_2}$, $\mathbf{F_3}$, … are associated with one single decryption key **B** satisfying $\boldsymbol{b}(\boldsymbol{f}(\mathbf{m}))=\mathbf{m}$ for any input **m** and for ***b*** being a decryption mechanism employing **B** and for ***f*** being an encryption mechanism employing any $\mathbf{F_i} \in \mathbf{F}$, comprising:

means for obtaining arbitrary and/or random input from which cryptographic keys are generated;

means for generating a decryption key;

means for generating one of a plurality of corresponding encryption keys;

means for supplying an encryptor with said encryption key;

means for accepting a message **m**;

means for encrypting **m** by said encryptor to ciphertext **c** using said encryption key;

means for supplying a decryptor with said decryption key; and

means for decrypting **c** by said decryptor to recover **m** using said decryption key.

16. A cryptographic system as in claim 15 comprising:

means for obtaining arbitrary and/or random input from which cryptographic keys are generated;

means for generating a decryption key including a set of parameters **p** in normal positional number representation;

means for generating a corresponding encryption key comprising:

means for converting **p** to self-contained components;

means for constructing encryption key parameters from said self-contained components by inserting zero or more arbitrary/random components in arbitrarily or randomly chosen component positions; and

means for generating all other encryption key parameters;

means for supplying an encryptor with said encryption key;

means for accepting a message **m**;

means for encrypting **m** by said encryptor to ciphertext **c** using said encryption key;

means for supplying a decryptor with said decryption key; and

means for decrypting **c** by said decryptor to recover **m** using said decryption key.

17. A cryptographic system, as in claim 15, with means for implementing **n** integer functions f_1, f_2, ..., f_n mapping from $[0, 2^h)$ to $[0, 2^h+\delta)$, where $\mathbf{h} > 1$ and $2^h+\delta > 1$, comprising:

means for obtaining arbitrary and/or random input from which cryptographic keys are generated;

means for generating a decryption key, including the generation of a first set of positive integers $\mathbf{X} = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n\}$ and a second set of positive integers $\mathbf{W} = \{\mathbf{w}_1, \mathbf{w}_2, \ldots,$

$\mathbf{w_n}\}$ satisfying $\mathbf{x_i} > \beta_1\mathbf{x_1} + \beta_2\mathbf{x_2} + \ldots + \beta_{i-1}\mathbf{x_{i-1}} + \gamma_1\mathbf{w_1} + \gamma_2\mathbf{w_2} + \ldots + \gamma_i\mathbf{w_i}$ where, for $1 \le \mathbf{i} \le \mathbf{n}$, $\gamma_i = f_i(\beta_i)$ and $\beta_i \in [0, 2^h)$;

means for transforming $\mathbf{X}$ to $\mathbf{Y} = \{\mathbf{y_1}, \mathbf{y_2}, \ldots, \mathbf{y_n}\}$ and $\mathbf{W}$ to $\mathbf{U} = \{\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_n}\}$, including an optional permutation and one or more rounds of invertible strong modular multiplication;

means for further transforming $\mathbf{Y}$ to $\mathbf{Z} = \{\mathbf{z_1}, \mathbf{z_2}, \ldots, \mathbf{z_n}\}$ and $\mathbf{U}$ to $\mathbf{V} = \{\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n}\}$ satisfying the following:

a. $\mathbf{p_0}, \mathbf{p_1}, \ldots, \mathbf{p_{t-1}}$ are pairwise co-prime

b. $\mathbf{z_i} = (\mathbf{z_{i,0}}, \mathbf{z_{i,1}}, \ldots, \mathbf{z_{i,qt-1}})$ for $1 \le \mathbf{i} \le \mathbf{n}$ and $\mathbf{q} \ge 1$

c. $\mathbf{J} = \{\mathbf{j_0}, \mathbf{j_1}, \ldots, \mathbf{j_{k-1}}\}$ is a set of arbitrary or random indices where $0 \le \mathbf{j_0}, \mathbf{j_2}, \ldots, \mathbf{j_{k-1}} < t$

d. $\mathbf{S} = \{\mathbf{s_0}, \mathbf{s_1}, \ldots, \mathbf{s_{k-1}}\}$ is an arbitrary or random set satisfying:

$0 \le \mathbf{s_0}, \mathbf{s_1}, \ldots, \mathbf{s_{k-1}} < \mathbf{qt}$, and $\mathbf{S} \% \mathbf{t} = \{\mathbf{s_0\%t}, \mathbf{s_1\%t}, \ldots, \mathbf{s_{k-1}\%t}\} = \mathbf{J}$

e. $\prod \mathbf{p_{j \in J}} > \beta_1\mathbf{y_1} + \beta_2\mathbf{y_2} + \ldots + \beta_n\mathbf{y_n} + \gamma_1\mathbf{u_1} + \gamma_2\mathbf{u_2} + \ldots + \gamma_n\mathbf{u_n}$

f. $\mathbf{z_{i,s \in S}} = \mathbf{y_i} \% \mathbf{p_{s\%t}}$

g. $\mathbf{z_{i,s \notin S}}$ are arbitrary or random numbers modulo $\mathbf{p_{s\%t}}$ for $0 \le \mathbf{s} < \mathbf{qt}$

h. $\mathbf{v_i} = (\mathbf{v_{i,0}}, \mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,qt-1}})$ for $1 \le \mathbf{i} \le \mathbf{n}$

i. $\mathbf{v_{i,s \in S}} = \mathbf{w_i} \% \mathbf{p_{s\%t}}$

j. $\mathbf{v_{i,s \notin S}}$ are arbitrary or random numbers modulo $\mathbf{p_{s\%t}}$ for $0 \le \mathbf{s} < \mathbf{qt}$.

18. A cryptographic system as in claim 17 further comprising:

means for supplying an encryptor with said encryption key;

means for encrypting by said encryptor one or more **nh**-bit data blocks which are divided into **h**-bit sub-blocks $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_n}$, where each block is encrypted to $\mathbf{c} = (\mathbf{c_0}, \mathbf{c_1}, \ldots, \mathbf{c_{qt-1}})$ with $\mathbf{c_s} = (\mathbf{d_1 z_{1,s}} + \mathbf{d_2 z_{2,s}} + \ldots + \mathbf{d_n z_{n,s}} + f_1(\mathbf{d_1})\mathbf{v_{1,s}} + f_2(\mathbf{d_2})\mathbf{v_{2,s}} + \ldots + f_n(\mathbf{d_n})\mathbf{v_{n,s}}) \% \mathbf{p_{s\%t}}$ for $0 \le \mathbf{s} < \mathbf{qt}$;

means for supplying a decryptor with said decryption key; and

means for decrypting by said decryptor each of said encrypted blocks **c** to recover said data blocks, by extracting $\mathbf{C} = \{\mathbf{c}_s \mid \mathbf{s} \in \mathbf{S}\}$ from **c** and by repeating, for each $\mathbf{d}_i$ for $1 \leq \mathbf{i} \leq \mathbf{n}$, the following:

a. converting **C** to a form where $\mathbf{d}_i$ can be determined

b. obtaining $\mathbf{d}_i$ from said converted **C**

c. removing from said converted **C** the quantity that $\mathbf{d}_i$ introduced.

19. A cryptographic system as in claim 18, where said encryption is carried out, in lieu, independently on self-contained components, comprising:

means for calculating **c** by carrying out two or more of said additions (+) and/or by computing two or more of said terms $\mathbf{d}_i\mathbf{z}_{i,j}$ and $f_i(\mathbf{d}_i)\mathbf{v}_{i,j}$ in parallel.

20. A cryptographic system, as in claim 15, for communicating a message securely from a first party **E** to a second party **D** comprising:

means for obtaining at party **D** arbitrary and/or random input from which cryptographic keys are generated;

means for generating at party **D** a decryption key to be kept secret;

means for generating at party **D** one of a plurality of corresponding encryption keys;

means for distributing said encryption key from party **D** to party **E**;

means for accepting a message **m** at party **E**;

means for encrypting **m** to ciphertext at party **E**, employing encryption key;

means for transmitting said ciphertext from party **E** to party **D**;

means for receiving said ciphertext at party **D**; and

means for decrypting said ciphertext at party **D** to recover **m**, employing said decryption key.